Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Brian
Last Name: Morin
Mailing Address: 7511W 136th Ln
City: Cedar Lake
Country: United States
State or Province: IN
ZIP/Postal Code: 46303
Email Address: agentbullvi@gmail.com
Organization Name: none
Comment: I would like to formally request that the FCC not implement rules and regulations that prohibit my ability to use devices I purchase the way I choose too. My choice to use open source software free of legal entanglement should not be curtailed; this is not how a free society should work.

I would like to formally request that the FCC not implement rules and regulations that prohibit my ability to use devices I purchase the way I choose too. My choice to use open source software free of legal entanglement should not be curtailed; this is not how a free society should work.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Tzvi
Last Name: Spitz
Mailing Address: 3 Johanna Lane
City: Monsey
Country: United States
State or Province: NY
ZIP/Postal Code: 10952
Email Address:
Organization Name:
Comment: Dear Sir or Ma'am,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Sincerely,
Tzvi

Dear Sir or Ma'am,

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Sincerely,
Tzvi

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Fred
Last Name: McDavid
Mailing Address: 62 Pine Top Rd
City: Fort Defiance
Country: United States
State or Province: VA
ZIP/Postal Code: 24437
Email Address: fred@hoppinfox.com
Organization Name:
Comment: As a professional software developer for the past 19 years and a casual developer for the past 34 years, I think it's important to point out that a regulation like this will likely 1) make the target devices much less secure for the general public and 2) make the target devices more complicated and, therefore, more prone to error and 3) cause the value of the target devices to decrease with the effectiveness of the manufacturer's compliance efforts.

<p>1) If companies' track record of support for aging devices remains as it has been, then the lack of updates will render devices increasingly insecure within 1.5 to 2 years after the date of manufacture. Note that, for many devices, the purchase will have taken place up to a year after the date of manufacture. Open-source projects like DD-WRT alleviate this problem by allowing an upgrade path beyond the date that manufacturers decide to stop releasing firmware for older models.

2) Complying with this regulation will require hardware updates which serve no functional purpose beyond legal compliance. To the software developer, these restrictions will take the form of hardware that won't perform as a rational engineer would expect. To the user, this will take the form of any of a number of possible glitches and/or security issues.

3) Since it will remain a good idea to update the firmware of these devices despite this short-sighted bit of regulation, there will be an increase in demand for the devices for which workarounds have been found which allow for modification. The devices which prove difficult to modify will find their way to the closets of the world as they become known for their growing list of discovered security holes. As an example, I always poke around looking for examples of someone's experience running Linux (an open-source operating system initially developed by non-commercial developers) on a given laptop model before I buy one and I always check that there is a way to run CyanogenMod (an open-source version of Android developed by non-commercial developers) on a smart phone before I buy it. This is pretty typical behavior for anyone technically minded enough to try it.

In summary, this is a terrible bit of regulation. Had it been passed a decade ago, it might well have prevented the emergence of the very devices it proposes to cripple. I sincerely hope the effort to pass this proposal fails.

As a professional software developer for the past 19 years and a casual developer for the past 34 years, I think it's important to point out that a regulation like this will likely 1) make the target devices much less secure for the general public and 2) make the target devices more complicated and, therefore, more prone to error and 3) cause the value of the target devices to decrease with the effectiveness of the manufacturer's compliance efforts.

<p>1) If companies' track record of support for aging devices remains as it has been, then the lack of updates will render

devices increasingly insecure within 1.5 to 2 years after the date of manufacture. Note that, for many devices, the purchase will have taken place up to a year after the date of manufacture. Open-source projects like DD-WRT alleviate this problem by allowing an upgrade path beyond the date that manufacturers decide to stop releasing firmware for older models.

2) Complying with this regulation will require hardware updates which serve no functional purpose beyond legal compliance. To the software developer, these restrictions will take the form of hardware that won't perform as a rational engineer would expect. To the user, this will take the form of any of a number of possible glitches and/or security issues.

3) Since it will remain a good idea to update the firmware of these devices despite this short-sighted bit of regulation, there will be an increase in demand for the devices for which workarounds have been found which allow for modification. The devices which prove difficult to modify will find their way to the closets of the world as they become known for their growing list of discovered security holes. As an example, I always poke around looking for examples of someone's experience running Linux (an open-source operating system initially developed by non-commercial developers) on a given laptop model before I buy one and I always check that there is a way to run CyanogenMod (an open-source version of Android developed by non-commercial developers) on a smart phone before I buy it. This is pretty typical behavior for anyone technically minded enough to try it.

In summary, this is a terrible bit of regulation. Had it been passed a decade ago, it might well have prevented the emergence of the very devices it proposes to cripple. I sincerely hope the effort to pass this proposal fails.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: chase
Last Name: tayrien
Mailing Address: 2805 n grant ave
City: springfield
Country: United States
State or Province: MO
ZIP/Postal Code: 65803
Email Address:
Organization Name:
Comment: I am against the motion from the FCC that would regulate and lockin firmware on most networking technology. This would stifle the economy when it comes to any networking technology manufactured in the US. Companies will take their business to other countries and sell these devices without the FCC to regulate it if this occurs. This would cost companies and yet again the American people. Technology needs to remain free and open for people to modify them if they will. PLEASE DO NOT ENFORCE THIS MOTION!!!

I am against the motion from the FCC that would regulate and lockin firmware on most networking technology. This would stifle the economy when it comes to any networking technology manufactured in the US. Companies will take their business to other countries and sell these devices without the FCC to regulate it if this occurs. This would cost companies and yet again the American people. Technology needs to remain free and open for people to modify them if they will. PLEASE DO NOT ENFORCE THIS MOTION!!!

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Josh
Last Name: Hudnall
Mailing Address: PO Box 2992
City: Grand Junction
Country: United States
State or Province: CO
ZIP/Postal Code: 81502
Email Address: joshhudnall@gmail.com
Organization Name:
Comment: I am writing to add my voice to the very large crowd that continues to say, do not restrict our freedoms. Business, security, economic and other concerns all come after freedom, never before. In the exceedingly rare circumstances that freedom must be reduced in the interest of some other concern, the burden falls on government to prove that such restrictions are both necessary and effective. Freedom is always assumed until it simply cannot be maintained in very specific and limited circumstances.

It is imperative that consumers be able to modify their devices in whatever way they see fitincluding installation of new software and/or operating systems on devicesin accordance with existing laws and regulations.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I am writing to add my voice to the very large crowd that continues to say, do not restrict our freedoms. Business, security, economic and other concerns all come after freedom, never before. In the exceedingly rare circumstances that freedom must be reduced in the interest of some other concern, the burden falls on government to prove that such restrictions are both necessary and effective. Freedom is always assumed until it simply cannot be maintained in very specific and limited circumstances.

It is imperative that consumers be able to modify their devices in whatever way they see fitincluding installation of new software and/or operating systems on devicesin accordance with existing laws and regulations.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and

companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Konstantin
Last Name: Lashuk
Mailing Address: konstantin.lashuk@gmail.com
City: Moscow
Country: Russia
State or Province: Moscow region
ZIP/Postal Code: 111396
Email Address:
Organization Name:
Comment: Don't do it

Don't do it

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Nathan
Last Name: Dial
Mailing Address: 1000 CR 474
City: Elgin
Country: United States
State or Province: TX
ZIP/Postal Code: 78621
Email Address: nathan.dial@gmail.com
Organization Name:
Comment: See attached file(s)

See attached file(s)

This applies particularly to Section A.b., particularly paragraph 20, where the measures would "ensure that certified equipment is not capable of operating with RF-controlling software for which it has not been approved". My understanding of this regulation is that by requiring wireless hardware to be incapable of operating with modified software, it not only prevents abusive software, but it also prevents wireless devices from operating customer-chosen, within-legal-limits software of our own choosing that replaces the manufacturer's software. **I would like to recommend the FCC, NOT implement this type of rule.**

To begin with, I am a computer programmer and a small-business entrepreneur. **The freedom to make** legal and safe **customizations** to wireless equipment **is of very real, tangible value** to small businesses that may be developing new products. It takes a lot of specialized knowledge to begin modifying this software, and the existing constraints built-in to customizable software on a wireless device already require education, and such education *always* includes an understanding of regulations and the penalties for violating them. There's not a big danger of accidentally going outside of what's regulated--and **for the few criminals who are interested in violating the law, there is very little to be done by a legal mandate that will stop them**. **New regulations will make things harder for honest, law-abiding entrepreneurs** and make very little difference among professional criminals, who will have the technology to break the laws regardless.

Second, I live in the country where quality Internet access is very difficult to obtain. This raises new challenges for me; challenges which I see new companies growing to meet with innovative new wireless products. **Making more wireless regulations makes it harder** for these new ISP's **to provide innovative services**, stifling what would be a bountiful blessing to (often poor) rural communities all over the United States.

And third but in some ways more important, I am a father of young children. The regulations that are being considered **will** not only **make it more difficult for my kids to get good Internet access**, which reduces their ability to learn from wonderful bandwidth-intensive educational resources like Khan Academy; it also, as they grow, **will reduce their ability** to experiment with new technologies, and **to become the innovative engineers driving America's future.**

The wealth of the Internet boom has been built on things that people can modify ourselves. It has made it easier to start a business, easier to improve things, and easier to learn. I have no problems with strict penalties for people who abuse their ability to customize products, to do things that are illegal--but these things are already illegal and they already have strict penalties. **Please do not** create new laws that make it impossible for law-abiding entrepreneurs, and engineers, teachers and students to modify their personally-owned hardware in safe, helpful and otherwise-legal ways.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Adam
Last Name: Chasen
Mailing Address: 827 E Hargett St
City: Raleigh
Country: United States
State or Province: NC
ZIP/Postal Code: 27601
Email Address: adam@chasen.name
Organization Name:
Comment: Please consider not restricting user modification from the host software side. While many systems may continue to have significant integration with System on Chips which include RF capabilities, it is important to be able to modify the *host* software portion of these systems to fix security holes in their devices when the manufacturer chooses to not do so. There are many high profile examples in the news.

Also consider not restricting modification from the RF side as well. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. There used to be an expectation from a device manufacturer and user that a portion of a burden of compliance reside on the manufacturer of the RF portion of a system from a fundamental silicon/construction/locked software level. Many of these systems are now driven by software. While it is convenient for these companies to unify the RF side with other OSI model levels, it is possible to construct these systems which allows user maintenance of OSI layers down to level 1 while enforcing FCC compliance.

This burden should be on RF manufacturers, not on end users through restrictions.

Please consider not restricting user modification from the host software side. While many systems may continue to have significant integration with System on Chips which include RF capabilities, it is important to be able to modify the *host* software portion of these systems to fix security holes in their devices when the manufacturer chooses to not do so. There are many high profile examples in the news.

Also consider not restricting modification from the RF side as well. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. There used to be an expectation from a device manufacturer and user that a portion of a burden of compliance reside on the manufacturer of the RF portion of a system from a fundamental silicon/construction/locked software level. Many of these systems are now driven by software. While it is convenient for these companies to unify the RF side with other OSI model levels, it is possible to construct these systems which allows user maintenance of OSI layers down to level 1 while enforcing FCC compliance.

This burden should be on RF manufacturers, not on end users through restrictions.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Rudolph
Last Name: Host
Mailing Address: 6509 175th St
City: Tinley Park
Country: United States
State or Province: IL
ZIP/Postal Code: 60477
Email Address:
Organization Name:
Comment: To whom it may concern,

I would like to advise against implementing any regulation that would lock down consumer wireless equipment against third party changes in software.

Preventing a consumer from having this freedom means that any security vulnerabilities that exist in a device may remain open if the manufacturer either can not or chooses to not release a new firmware image. Open source firmware, such as OpenWRT, gives individuals the opportunity to patch any vulnerabilities on their own terms without having to rely on the vendor to do so.

Researchers also depend on the need to run modified software on their devices. Taking this ability away may make it difficult or impossible to conduct the experimentation required to innovate or find and patch vulnerabilities in existing software.

Amateur radio operators share a portion of the radio spectrum with WiFi and other consumer wireless devices. Many amateur radio operators utilize consumer equipment as an inexpensive way to access this portion of the spectrum. Locking devices down will prevent licensed individuals from being able to use their equipment, even in ways that they are legally allowed to do so.

Ultimately, the actions that you are trying to prevent are already against the law. Instead of trying to come up with a solution with many drawbacks, it would be better to enforce the existing regulations and pursue the individuals that are in violation.

Thank you,
Rudolph Host

To whom it may concern,

I would like to advise against implementing any regulation that would lock down consumer wireless equipment against third party changes in software.

Preventing a consumer from having this freedom means that any security vulnerabilities that exist in a device may remain open if the manufacturer either can not or chooses to not release a new firmware image. Open source firmware, such as OpenWRT, gives individuals the opportunity to patch any vulnerabilities on their own terms without having to

rely on the vendor to do so.

Researchers also depend on the need to run modified software on their devices. Taking this ability away may make it difficult or impossible to conduct the experimentation required to innovate or find and patch vulnerabilities in existing software.

Amateur radio operators share a portion of the radio spectrum with WiFi and other consumer wireless devices. Many amateur radio operators utilize consumer equipment as an inexpensive way to access this portion of the spectrum. Locking devices down will prevent licensed individuals from being able to use their equipment, even in ways that they are legally allowed to do so.

Ultimately, the actions that you are trying to prevent are already against the law. Instead of trying to come up with a solution with many drawbacks, it would be better to enforce the existing regulations and pursue the individuals that are in violation.

Thank you,
Rudolph Host

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Amos
Last Name: Petersen
Mailing Address: 926 S Van Buren St.
City: Iowa City
Country: United States
State or Province: IA
ZIP/Postal Code: 52240
Email Address: subepsilon@gmail.com
Organization Name: Eccocast R&D
Comment: I am an electrical engineer and radio experimenter. In order to innovate and improve upon current wifi technologies (such as the current 802.11s standards for wireless mesh networking), I need to be able to flash open-source firmware to wifi transcievers. Passing this rule will KILL innovation in the US and prevent people like me from contributing to our technological advancement. Those experimenters involved in wireless data transmission and radio will leave the USA for countries with less prohibitive and intrusive rules and will leave our country at a significant disadvantage in the race to develop superior computing and networking technologies.

Please do not restrict firmware changes as planned; instead think about enforcement of existing laws which already prohibit use of certain unlicensed frequencies beyond a certain ERP, etc.

DON"T KILL INNOVATION!

I am an electrical engineer and radio experimenter. In order to innovate and improve upon current wifi technologies (such as the current 802.11s standards for wireless mesh networking), I need to be able to flash open-source firmware to wifi transcievers. Passing this rule will KILL innovation in the US and prevent people like me from contributing to our technological advancement. Those experimenters involved in wireless data transmission and radio will leave the USA for countries with less prohibitive and intrusive rules and will leave our country at a significant disadvantage in the race to develop superior computing and networking technologies.

Please do not restrict firmware changes as planned; instead think about enforcement of existing laws which already prohibit use of certain unlicensed frequencies beyond a certain ERP, etc.

DON"T KILL INNOVATION!

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Josh
Last Name: Matchuny
Mailing Address: 26 sugar creek lane
City: glenarm
Country: United States
State or Province: IL
ZIP/Postal Code: 62536
Email Address: null
Organization Name: null
Comment: The products we purchase should be ours to do what we feel the need to. Inacting this will only lead to more and more regulations regarding the use of our devices and in a way slowly killing off some innovation.

The products we purchase should be ours to do what we feel the need to. Inacting this will only lead to more and more regulations regarding the use of our devices and in a way slowly killing off some innovation.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Terry
Last Name: Hardie
Mailing Address: 228 Appian Way
City: Union City
Country: United States
State or Province: CA
ZIP/Postal Code: 94587
Email Address: terryh@orcas.net
Organization Name:
Comment: Limiting user installation of custom software on WiFi routers would significantly stifle innovation in this sector. The general poor quality of vendor supplied software in WiFi routers gives the open source community a significant role in providing software for these devices to make them reliable and far more useful. Vendor supplied software is often buggy and woefully lacking in features. Open source software provides significant value for these devices.

The number of users who are able to modify this software to violate FCC rules is so insignificant, and the people able to do this would continue to even if rules were put in place to limit user modifications to WiFi routers.

Terry Hardie
FCC Amateur radio general license holder KW0RCA & Software engineer

Limiting user installation of custom software on WiFi routers would significantly stifle innovation in this sector. The general poor quality of vendor supplied software in WiFi routers gives the open source community a significant role in providing software for these devices to make them reliable and far more useful. Vendor supplied software is often buggy and woefully lacking in features. Open source software provides significant value for these devices.

The number of users who are able to modify this software to violate FCC rules is so insignificant, and the people able to do this would continue to even if rules were put in place to limit user modifications to WiFi routers.

Terry Hardie
FCC Amateur radio general license holder KW0RCA & Software engineer

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Ken
Last Name: Welker
Mailing Address: 305 N. Knollwood Drive, Suite 5103
City: Blacksburg
Country: United States
State or Province: VA
ZIP/Postal Code: 24060
Email Address: kenvwelker@gmail.com
Organization Name:
Comment: Good afternoon. Regarding the proposed changes to the regulations on wireless devices, I respectfully encourage you to allow installations of modified firmware, provided that the transmitting power and other important capabilities be restricted to no more than legal limits through a separate chip. In this manner, the FCC may continue to manage wireless capabilities of devices as they have done for decades.

Additionally, this will allow technical consumers the option to perform their own firmware installations in order to fix problems, including security issues, which the manufacturers are unable or unwilling to address.

Vulnerable routers with unsupported firmware are a large problem on the Internet; http://www.forbes.com/sites/thomasbrewster/2015/05/19/home-routers-vulnerable-to-netusb-attack/ and http://www.pcmag.com/article2/0,2817,2490566,00.asp are links to just two examples of many. Frequently these devices are only a few years old, and have many years of useful life remaining; however, because the manufacturer no longer provides updates for whatever reason, the devices may be subject to being taken over by malicious remote users and employed in botnets, distributed denial-of-service attacks, cybercrime proxies, and other malicious activities not intended by the owner.

It's not always an option to buy a new wireless device every time a problem pops up that a manufacturer won't fix. Those on limited incomes, especially students, and/or those that are just unwilling to throw away devices that are still useful, would welcome the opportunity to either fix their devices or have someone else fix these for them.

Thank you for the opportunity to comment.

Good afternoon. Regarding the proposed changes to the regulations on wireless devices, I respectfully encourage you to allow installations of modified firmware, provided that the transmitting power and other important capabilities be restricted to no more than legal limits through a separate chip. In this manner, the FCC may continue to manage wireless capabilities of devices as they have done for decades.

Additionally, this will allow technical consumers the option to perform their own firmware installations in order to fix problems, including security issues, which the manufacturers are unable or unwilling to address.

Vulnerable routers with unsupported firmware are a large problem on the Internet; http://www.forbes.com/sites/thomasbrewster/2015/05/19/home-routers-vulnerable-to-netusb-attack/ and http://www.pcmag.com/article2/0,2817,2490566,00.asp are links to just two examples of many. Frequently these devices are only a few years old, and have many years of useful life remaining; however, because the manufacturer no

longer provides updates for whatever reason, the devices may be subject to being taken over by malicious remote users and employed in botnets, distributed denial-of-service attacks, cybercrime proxies, and other malicious activities not intended by the owner.

It's not always an option to buy a new wireless device every time a problem pops up that a manufacturer won't fix. Those on limited incomes, especially students, and/or those that are just unwilling to throw away devices that are still useful, would welcome the opportunity to either fix their devices or have someone else fix these for them.

Thank you for the opportunity to comment.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: chris
Last Name: giesen
Mailing Address: 61 hampton street
City: bridgeton
Country: United States
State or Province: NJ
ZIP/Postal Code: 08302
Email Address:
Organization Name:
Comment: I feel it would be a huge mistake to block alternative firmware from consumer routers. For years us ham radio operators have tinkered with radios and it has helped technology to grown in the united states. The same goes with firmware like ddwrt we are seeing much more stable routers with features that normally would only been seen on a extremely expensive commercial router. Blocking opensource firmware in the usa will not stop the problem of people abusing power limits on 2.4 ghz hardware, people will just start buying cheap hardware from china that may even splatter over into other restricted bands. With the spread of 4g cellular data I feel the wifi warriors of the past have moved on and those that use to abuse the limits of wifi power will just use cellular data now and those of us still running opensource software on our routers will be doing it to learn more about the equipment and customize it to our needs rather then to abuse power limits.

I feel it would be a huge mistake to block alternative firmware from consumer routers. For years us ham radio operators have tinkered with radios and it has helped technology to grown in the united states. The same goes with firmware like ddwrt we are seeing much more stable routers with features that normally would only been seen on a extremely expensive commercial router. Blocking opensource firmware in the usa will not stop the problem of people abusing power limits on 2.4 ghz hardware, people will just start buying cheap hardware from china that may even splatter over into other restricted bands. With the spread of 4g cellular data I feel the wifi warriors of the past have moved on and those that use to abuse the limits of wifi power will just use cellular data now and those of us still running opensource software on our routers will be doing it to learn more about the equipment and customize it to our needs rather then to abuse power limits.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Perry
Last Name: Smith
Mailing Address: 225 parkdale ave
City: buffalo
Country: United States
State or Province: NY
ZIP/Postal Code: 14213
Email Address: pvsmith2@gmail.com
Organization Name:
Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. Wireless networking research depends on the ability of researchers to investigate and modify their devices. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Aaron
Last Name: Carlton
Mailing Address: 2829 Cliffside Drive
City: Christiana
Country: United States
State or Province: TN
ZIP/Postal Code: 37037
Email Address: uid89626@gmail.com
Organization Name:
Comment: Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The future of free humanity depends on open and modifyable devices. Do you know know with absolute certainty what we need tomorrow?
Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please do not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The future of free humanity depends on open and modifyable devices. Do you know know with absolute certainty what we need tomorrow?
Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Ted
Last Name: Pohler
Mailing Address: 4488 Summertime Ct. SE
City: Grand Rapids
Country: United States
State or Province: MI
ZIP/Postal Code: 49508
Email Address:
Organization Name:
Comment: You need to do this in a way that doesn't preclude people from modifications to their own WiFi routers. I don't see the benefit of limitations here in general, but there are clear cases where the limitations are not considering cases where they should not apply.

You need to do this in a way that doesn't preclude people from modifications to their own WiFi routers. I don't see the benefit of limitations here in general, but there are clear cases where the limitations are not considering cases where they should not apply.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: michael
Last Name: nargang
Mailing Address: 621 s king street
City: seattle
Country: United States
State or Province: WA
ZIP/Postal Code: 98104
Email Address:
Organization Name:
Comment: This is bad. Device manufacturers have already demonstrated they cannot keep secure up to date firmware on home network devices. Also if this interferes with open smartphone development who knows what we'll lose.

This is bad. Device manufacturers have already demonstrated they cannot keep secure up to date firmware on home network devices. Also if this interferes with open smartphone development who knows what we'll lose.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Andrey
Last Name: Parinov
Mailing Address: aparinov@gmail.com
City: Moscow
Country: Russia
State or Province: Moscow
ZIP/Postal Code: 0000111250
Email Address: savelevamarin@gmail.com
Organization Name: National Research University Moscow Power Engineering Institute
Comment: Please don't accept this proposal.

Please don't accept this proposal.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Chris
Last Name: Vander Kolk
Mailing Address: 15729 Holly Grove Rd
City: Silver Spring
Country: United States
State or Province: MD
ZIP/Postal Code: 20905
Email Address: astro128@yahoo.com
Organization Name:
Comment: Please do not ban the modification of WIFI router firmware. I have successfully running a modified firmware for years now and it has greatly increased its abilities. Further, as we head deeper in a constantly monitored, privacy averse world, I appreciate the ability to overwrite the routers firmware to keep unwanted privacy intrusion out of my home. It is my equipment and should be able to disable features on it that I do not want. And if the company's software/firmware does not allow this then innately, then using my custom firmware is my only recourse.

Please do not take our right to control our equipment away. It provides a necessary check and balance against the product manufacturers.

Thank you for your time,
Chris

Please do not ban the modification of WIFI router firmware. I have successfully running a modified firmware for years now and it has greatly increased its abilities. Further, as we head deeper in a constantly monitored, privacy averse world, I appreciate the ability to overwrite the routers firmware to keep unwanted privacy intrusion out of my home. It is my equipment and should be able to disable features on it that I do not want. And if the company's software/firmware does not allow this then innately, then using my custom firmware is my only recourse.

Please do not take our right to control our equipment away. It provides a necessary check and balance against the product manufacturers.

Thank you for your time,
Chris

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Trevor
Last Name: Bossert
Mailing Address: 1562 Autumn Valley Way
City: Brentwood
Country: United States
State or Province: CA
ZIP/Postal Code: 94513
Email Address: alanboss@gmail.com
Organization Name:
Comment: Regulating this area provides no benefit. Hardware capabilities can be regulated, but setting a precedent of what software a person can run on their own equipment is bad for innovation. Please do not regulate firmware on wifi devices.

Regulating this area provides no benefit. Hardware capabilities can be regulated, but setting a precedent of what software a person can run on their own equipment is bad for innovation. Please do not regulate firmware on wifi devices.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Brendan
Last Name: Foley
Mailing Address: 12102 Foley St
City: Silver Spring
Country: United States
State or Province: MD
ZIP/Postal Code: 20902
Email Address: djindy@gmail.com
Organization Name:
Comment: Please do not take away the ability of users/owners of devices to install the software of their choosing on their own devices.

Please do not take away the ability of users/owners of devices to install the software of their choosing on their own devices.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: G. Ralph
Last Name: Kuntz, MD
Mailing Address: 8720 SW 103rd Ave.
City: Gainesville
Country: United States
State or Province: FL
ZIP/Postal Code: 32608
Email Address:
Organization Name:
Comment: Please do not ban the installation of new firmware in WiFi routers. Many people prefer to use one of the open source alternatives to the manufacturers' own offerings. Since the routers have already been purchased, this results in no lost revenue to the manufacturers.

Please do not ban the installation of new firmware in WiFi routers. Many people prefer to use one of the open source alternatives to the manufacturers' own offerings. Since the routers have already been purchased, this results in no lost revenue to the manufacturers.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Lee
Last Name: Keitel
Mailing Address: 333 Riviera Dr.
City: Mt. Vernon
Country: United States
State or Province: IN
ZIP/Postal Code: 47620-1255
Email Address:
Organization Name:
Comment: I respectfully request that the FCC not implement any regulations that would prohibit the ability for uses to install/modify the software of their choosing on their computing devices as outlined in "Equipment Authorization and Electronic Labeling for Wireless Devices". Research into new and innovative wireless networking depends on the ability of researchers to investigate and modify their devices and software. Americans especially need the ability to fix security holes in their devices when the manufactures choose not to do so. In the past, users have been able to fix countless bugs and security problems but only because they were able to modify their devices. Billions of dollars of commerce depends on the ability of users and companies to install software on their wireless devices as they see fit. Will people break the rules? Of course they will. And those people should be punished through fines and other appropriate measures. But the incorrect actions of the few should force the rest of regulatory-abiding users to be restricted. So again I ask, please do not implement these proposed rules. They will only hurt the end user. Not help.

I respectfully request that the FCC not implement any regulations that would prohibit the ability for uses to install/modify the software of their choosing on their computing devices as outlined in "Equipment Authorization and Electronic Labeling for Wireless Devices". Research into new and innovative wireless networking depends on the ability of researchers to investigate and modify their devices and software. Americans especially need the ability to fix security holes in their devices when the manufactures choose not to do so. In the past, users have been able to fix countless bugs and security problems but only because they were able to modify their devices. Billions of dollars of commerce depends on the ability of users and companies to install software on their wireless devices as they see fit. Will people break the rules? Of course they will. And those people should be punished through fines and other appropriate measures. But the incorrect actions of the few should force the rest of regulatory-abiding users to be restricted. So again I ask, please do not implement these proposed rules. They will only hurt the end user. Not help.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jonathan
Last Name: Huff
Mailing Address: 1748 W 900 S
City: Spanish Fork
Country: United States
State or Province: UT
ZIP/Postal Code: 84660
Email Address: zarcos@gmail.com
Organization Name:
Comment: Thank you for this request for comment.

I would like to request that the FCC reconsider the proposed changes. Specifically, any changes that restrict the ability of the users of the equipment to make necessary changes to their FCC regulated equipment is anti-competitive and ultimately harmful to the research, development, manufacture and use of FCC regulated devices. Restricting the installation and modification of the code that interfaces with FCC regulated devices and FCC regulated frequencies of all kinds may, in fact reduce the incidence of "rogue" devices that act against FCC regulation, but at the expense of every other legitimate use of FCC regulated devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Obviously, doing this responsibly requires precautions to act within FCC regulation, but if these precautions are met, it must not be illegal for them to modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This can happen for many reasons: manufacturers go out of business, it's not cost effective for them to issue patches for what are often very costly vulnerabilities, or any of many other possible reasons. The user is ultimately legally responsible if the device misbehaves according to FCC regulation, and therefore it is absolutely necessary that the user be able to change and control this behavior at need.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing, not to mention the security of any companies that use FCC regulated devices for mission critical deployments.

Thank you for this request for comment.

I would like to request that the FCC reconsider the proposed changes. Specifically, any changes that restrict the ability of the users of the equipment to make necessary changes to their FCC regulated equipment is anti-competitive and ultimately harmful to the research, development, manufacture and use of FCC regulated devices. Restricting the installation and modification of the code that interfaces with FCC regulated devices and FCC regulated frequencies of all kinds may, in fact reduce the incidence of "rogue" devices that act against FCC regulation, but at the expense of every other legitimate use of FCC regulated devices.

Wireless networking research depends on the ability of researchers to investigate and modify their devices. Obviously, doing this responsibly requires precautions to act within FCC regulation, but if these precautions are met, it must not be illegal for them to modify their devices.

Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so. This can happen for many reasons: manufacturers go out of business, it's not cost effective for them to issue patches for what are often very costly vulnerabilities, or any of many other possible reasons. The user is ultimately legally responsible if the device misbehaves according to FCC regulation, and therefore it is absolutely necessary that the user be able to change and control this behavior at need.

Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.

Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing, not to mention the security of any companies that use FCC regulated devices for mission critical deployments.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Robert
Last Name: Serrano
Mailing Address: 1322 Serene Dr.
City: Erie
Country: United States
State or Province: CO
ZIP/Postal Code: 80516
Email Address: hoyasaxa84@sbcglobal.net
Organization Name:
Comment: I request that you not implement rules that take away the ability of users to install the software of their choosing on their computer equipment. As an American, I feel that if I've paid for a product, I have the right to install whatever software I want as long as it does no harm to others. To make a rule contrary to this is an infringement of individual rights.

Also:
1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Thank you for your consideration.

I request that you not implement rules that take away the ability of users to install the software of their choosing on their computer equipment. As an American, I feel that if I've paid for a product, I have the right to install whatever software I want as long as it does no harm to others. To make a rule contrary to this is an infringement of individual rights.

Also:
1. Wireless networking research depends on the ability of researchers to investigate and modify their devices.
2. Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
3. Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
4. Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Thank you for your consideration.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Link
Last Name: Porterfield
Mailing Address: 823 Blaine St #423
City: Caldwell
Country: United States
State or Province: ID
ZIP/Postal Code: 83605-3733
Email Address: link+fcc.wifi@qpg.us
Organization Name: QPG, Ltd. Co.
Comment: As a licensed ham operator as well as a networking professional whose livelihood is very involved with open source software and communications devices, I respectfully request the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

The impact of this rule will have far reaching effects on economics, innovation and network security. Access to custom firmware has led to fixed software bugs and patched security vulnerabilities that would otherwise be left to languish by commodity oriented vendors that have less incentive to fix such shortcomings than the actual operators of the devices.

Secure WiFi vendors and retail hotspot vendors depend on being able to load custom firmware on networking equipment, as do wireless networking researchers.

Public safety will also be negatively impacted by these proposed rule changes as mesh network projects like Broadband-Hamnet (http://www.broadband-hamnet.org) will be rendered unusable as they depend on the ability to load custom firmware on equipment.

For the sake of the economy, technological innovation, network security and public safety, I must request these proposed rules not be implemented.

As a licensed ham operator as well as a networking professional whose livelihood is very involved with open source software and communications devices, I respectfully request the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices.

The impact of this rule will have far reaching effects on economics, innovation and network security. Access to custom firmware has led to fixed software bugs and patched security vulnerabilities that would otherwise be left to languish by commodity oriented vendors that have less incentive to fix such shortcomings than the actual operators of the devices.

Secure WiFi vendors and retail hotspot vendors depend on being able to load custom firmware on networking equipment, as do wireless networking researchers.

Public safety will also be negatively impacted by these proposed rule changes as mesh network projects like Broadband-Hamnet (http://www.broadband-hamnet.org) will be rendered unusable as they depend on the ability to load custom firmware on equipment.

For the sake of the economy, technological innovation, network security and public safety, I must request these

proposed rules not be implemented.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Daniel
Last Name: Drown
Mailing Address: 4909 Craig Drive
City: Austin
Country: United States
State or Province: TX
ZIP/Postal Code: 78727
Email Address: dan-fcc@drown.org
Organization Name:
Comment: Hello, I am a software developer with an interest in software on both the mobile phone and the consumer wifi access point hardware. I developed the 464xlat standard in use by all of T-Mobile's Android and Windows phones today because I was able to modify my mobile phone OS as well as my wifi access point software. I fear these changes will negatively impact my ability to do this kind of work in the future.

Additionally, this change in the rules will affect the wireless industry as a whole negatively. Currently, the mobile phone and consumer wifi access point industry makes their development investment before launching their devices. After a device has been launched, the amount of money invested in developing security fixes, bug fixes, and feature improvements is reduced to the absolute minimum. The open source community has taken it upon themselves to maintain older devices. Examples of groups doing this are CyanogenMod for the phone and OpenWRT for the access point. Without these groups, phones and access points no longer seen as a reasonable development investment by the company that sells them would have no security or bug fixes.

Beyond the development of fixes for known security flaws, there's also the identification of previously unknown security flaws. When the code running on these devices can't be modified by a third party, it won't get the attention or more importantly the code auditing it currently does. Without the ability to change the code running, the only people that would work on the code would either be working for a company focused on short term profit or looking specifically to profit off of security issues. Both groups have an interest in not fixing security problems, especially ones not widely known. The former group because it's an expense with no garantee of profit and the latter group because it's a new flaw they can sell to interested parties.

Because of these issues, I hope you will reconsider this ruling.

Hello, I am a software developer with an interest in software on both the mobile phone and the consumer wifi access point hardware. I developed the 464xlat standard in use by all of T-Mobile's Android and Windows phones today because I was able to modify my mobile phone OS as well as my wifi access point software. I fear these changes will negatively impact my ability to do this kind of work in the future.

Additionally, this change in the rules will affect the wireless industry as a whole negatively. Currently, the mobile phone and consumer wifi access point industry makes their development investment before launching their devices. After a device has been launched, the amount of money invested in developing security fixes, bug fixes, and feature improvements is reduced to the absolute minimum. The open source community has taken it upon themselves to maintain older devices. Examples of groups doing this are CyanogenMod for the phone and OpenWRT for the access point. Without these groups, phones and access points no longer seen as a reasonable development investment by the

company that sells them would have no security or bug fixes.

Beyond the development of fixes for known security flaws, there's also the identification of previously unknown security flaws. When the code running on these devices can't be modified by a third party, it won't get the attention or more importantly the code auditing it currently does. Without the ability to change the code running, the only people that would work on the code would either be working for a company focused on short term profit or looking specifically to profit off of security issues. Both groups have an interest in not fixing security problems, especially ones not widely known. The former group because it's an expense with no garantee of profit and the latter group because it's a new flaw they can sell to interested parties.

Because of these issues, I hope you will reconsider this ruling.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Scott
Last Name: Waun
Mailing Address: 8065 Vegas Circle
City: West Chester
Country: United States
State or Province: OH
ZIP/Postal Code: 45069
Email Address: nospam@waun.net
Organization Name: Concerned citizen
Comment: Please reconsider this action... it is far too dramatic a response to a limited-scope problem. Open platforms drive innovation, which drives growth. Additionally, openness leads to security, as vulnerabilities can be patched by anyone, well beyond the typical support period of many manufacturers.

Don't move progress backward by adopting this rule!

Please reconsider this action... it is far too dramatic a response to a limited-scope problem. Open platforms drive innovation, which drives growth. Additionally, openness leads to security, as vulnerabilities can be patched by anyone, well beyond the typical support period of many manufacturers.

Don't move progress backward by adopting this rule!

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Arseniy
Last Name: Barinov
Mailing Address: Gromadyanska 2b, kv 3.
City: Irpin
Country: Ukraine
State or Province: Kiyvskaya ob
ZIP/Postal Code: 08205
Email Address: Arseny1@ukr.net
Organization Name:
Comment: Let me do with my property what I want.

Let me do with my property what I want.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: James
Last Name: Smith
Mailing Address: 12726 Castle Bend
City: San Antonio
Country: United States
State or Province: TX
ZIP/Postal Code: 78230
Email Address: james@apertum.org
Organization Name:
Comment: I am opposed to the changes that will require manufacturers to further lock down the software of their devices.

Forcing hardware manufacturers to further restrict these wireless devices will do more harm than good when considering all of the factors. Manufacturers will not take security threats/holes any more seriously with these new restrictions. In fact, it's likely they will simply ignore them. The ability to modify devices we own is essential to maintaining peace of mind. Very few people make any modifications at all to most things they interact with. An even smaller number of people even understand that these devices can be modified. By enforcing these restrictions, the only people that will be affected are the ones making harmless modifications to devices they own.

Thanks for your time.

I am opposed to the changes that will require manufacturers to further lock down the software of their devices.

Forcing hardware manufacturers to further restrict these wireless devices will do more harm than good when considering all of the factors. Manufacturers will not take security threats/holes any more seriously with these new restrictions. In fact, it's likely they will simply ignore them. The ability to modify devices we own is essential to maintaining peace of mind. Very few people make any modifications at all to most things they interact with. An even smaller number of people even understand that these devices can be modified. By enforcing these restrictions, the only people that will be affected are the ones making harmless modifications to devices they own.

Thanks for your time.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: James
Last Name: Johnson
Mailing Address: 6054 Camino Manzano
City: Anaheim
Country: United States
State or Province: CA
ZIP/Postal Code: 92807
Email Address:
Organization Name:
Comment: Stop making more rules. If I want to modify my computer, WiFi router, etc, then I should be able to. The more rules there are, the less freedom there is. This proposed measure will stifle creativity and set us back decades in progress. Also this hurts all those who make a living developing in modified systems. Just drop this measure and focus on the real issues at hand, like Comcast and similar companies charging way more to Americans than say, Germans who pay much less for internet access.

Stop making more rules. If I want to modify my computer, WiFi router, etc, then I should be able to. The more rules there are, the less freedom there is. This proposed measure will stifle creativity and set us back decades in progress. Also this hurts all those who make a living developing in modified systems. Just drop this measure and focus on the real issues at hand, like Comcast and similar companies charging way more to Americans than say, Germans who pay much less for internet access.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Kyle
Last Name: Falconer
Mailing Address: 1034 Foxchase Dr #345
City: San Jose
Country: United States
State or Province: CA
ZIP/Postal Code: 95123
Email Address: kfalconer@gmail.com
Organization Name:
Comment: I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The following are some of the reasons why this rule should not be implemented:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices.
-Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
-Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
-Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

I respectfully ask the FCC to not implement rules that take away the ability of users to install the software of their choosing on their computing devices. The following are some of the reasons why this rule should not be implemented:

-Wireless networking research depends on the ability of researchers to investigate and modify their devices.
-Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
-Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
-Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Gregor
Last Name: Glashuettner
Mailing Address: Gregory me one party.at
City: Vienna
Country: Austria
State or Province: Vienna
ZIP/Postal Code: 1020
Email Address: gregor@meineparty.at
Organization Name: Unwired Networks GmbH
Comment: The free use of the ISM band had a huge positive economic effect, even more by means of open source software. The proposal in question would ruin the benefits altogether.

The free use of the ISM band had a huge positive economic effect, even more by means of open source software. The proposal in question would ruin the benefits altogether.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: James
Last Name: Pearce
Mailing Address: 42 Wallaby Way
City: Sidney
Country: Australia
State or Province: New South Wales
ZIP/Postal Code: 2000
Email Address:
Organization Name:
Comment: This is why nothing is made in America anymore.

This is why nothing is made in America anymore.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Matthew
Last Name: Knapp
Mailing Address: 10801 Heather Ridge Cir
City: Orlando
Country: United States
State or Province: FL
ZIP/Postal Code: 32817
Email Address: linkmaster6@gmail.com
Organization Name:
Comment: Hello my Name is Matthew Knapp and I must implore you not to implement this rule. This takes away the consumers right to decide what type of software a user chooses to use. I know that I personally use modified routers to patch security problems in my router that the manufacture has decided to abandon. Please do not do this the idea is a bad one.

Hello my Name is Matthew Knapp and I must implore you not to implement this rule. This takes away the consumers right to decide what type of software a user chooses to use. I know that I personally use modified routers to patch security problems in my router that the manufacture has decided to abandon. Please do not do this the idea is a bad one.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Jonathan
Last Name: Hanson
Mailing Address: 2801 E 120th Ave
City: Thornton
Country: United States
State or Province: CO
ZIP/Postal Code: 80233
Email Address: jonhanson1987@gmail.com
Organization Name:
Comment: Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Wireless networking research depends on the ability of researchers to investigate and modify their devices.
Americans need the ability to fix security holes in their devices when the manufacturer chooses to not do so.
Users have in the past fixed serious bugs in their wifi drivers, which would be banned under the NPRM.
Billions of dollars of commerce, such as secure wifi vendors, retail hotspot vendors, depends on the ability of users and companies to install the software of their choosing.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Dougal
Last Name: Campbell
Mailing Address: 822 Holly Ridge
City: Canton
Country: United States
State or Province: GA
ZIP/Postal Code: 30115
Email Address: dougal.campbell@gmail.com
Organization Name:
Comment: Regarding ET Docket No. 15-170; RM-11673, which proposes to require manufactures to lock down wireless transmitters so that they can not be re-programmed by end users --

Please consider the slippery slope of unintended consequences, stifling of innovation, and chilling effect that this action could have. Since many existing and in-development products use components commonly called a System on a Chip (SoC) which combines a radio with a programmable microprocessor or microcontroller, the ability for a technical end-user to perform their own upgrades or replacement of firmware to re-purpose a device would be halted.

While this probably seems like a pretty rare thing, this has often been a source of innovation which has been the genesis of new products or has breathed new life into old ones. Projects like OpenWRT, for example, allow users to reprogram many consumer-level WiFi routers with new firmware which not only offers improved functionality, but also improves security over the original programming from the manufacturer (who, in many cases, have stopped providing updates for said device).

These changes would probably also make it harder for security researchers to analyze and test products. Security research often uncovers vulnerabilities not predicted by manufacturers. Independent researchers are a resource that many companies are coming to appreciate more, and this kind of research can sometimes be the only way that the public becomes aware of problems that some companies might prefer to quietly sweep under the rug, pretending that no problem exists, while consumers continue to suffer the consequences.

Regarding ET Docket No. 15-170; RM-11673, which proposes to require manufactures to lock down wireless transmitters so that they can not be re-programmed by end users --

Please consider the slippery slope of unintended consequences, stifling of innovation, and chilling effect that this action could have. Since many existing and in-development products use components commonly called a System on a Chip (SoC) which combines a radio with a programmable microprocessor or microcontroller, the ability for a technical end-user to perform their own upgrades or replacement of firmware to re-purpose a device would be halted.

While this probably seems like a pretty rare thing, this has often been a source of innovation which has been the genesis of new products or has breathed new life into old ones. Projects like OpenWRT, for example, allow users to reprogram many consumer-level WiFi routers with new firmware which not only offers improved functionality, but also improves security over the original programming from the manufacturer (who, in many cases, have stopped providing updates for said device).

These changes would probably also make it harder for security researchers to analyze and test products. Security research often uncovers vulnerabilities not predicted by manufacturers. Independent researchers are a resource that many companies are coming to appreciate more, and this kind of research can sometimes be the only way that the public becomes aware of problems that some companies might prefer to quietly sweep under the rug, pretending that no problem exists, while consumers continue to suffer the consequences.

Please Do Not Reply To This Email.

Public Comments on Equipment Authorization and Electronic Labeling for Wireless Devices:========

Title: Equipment Authorization and Electronic Labeling for Wireless Devices
FR Document Number: 2015-18402
RIN:
Publish Date: 8/6/2015 12:00:00 AM

Submitter Info:
First Name: Braxton
Last Name: Story
Mailing Address: 3933 Ariel Ave
City: Gillette
Country: United States
State or Province: WY
ZIP/Postal Code: 82718
Email Address:
Organization Name: Protech Computing Services LLC
Comment: I believe this to be a bad idea for the following reasons:

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Thanks,

Braxton.

I believe this to be a bad idea for the following reasons:

Innovation

Innovation in network and wireless technology depends on the ability to experiment with software and hardware at the deepest levels. CeroWrt, an open source router firmware, developed a fix for an important form of network congestion called Bufferbloat. This fix is was added to the Linux kernel to be used by the billions of users of Linux. HNCP, a proposed IETF proposed standard for managing home networks, is being developed using OpenWrt. Mesh networking technologies for developing stable distributed internet access are regularly implemented on OpenWrt and much research and implementation on mesh networking has occurred outside of manufacturers. Nearly 7,200 scholarly articles on wireless networking technologies reference a particular brand of open and modifiable hardware which would be banned under these rules. Without the ability to change the software on the device, these innovations would not have occurred. The innovations done by the community are later often picked up by the home router vendors and being integrated into their normal firmware versions for their next generations of devices.

Economic Impact

Millions of dollars of economic activity depend on third-party firmware. Major semiconductor and wireless hardware manufacturers use OpenWrt as the base of their router software.[1][2][3][4][5] At the same time, OpenWrt is managed and developed primarily by a community of individuals modifying their own routers and installing customized versions of OpenWrt on their own routers. Sometimes these routers originally had OpenWrt on them while others did not. Strong

industry-community collaboration reduces the costs of maintenance and increases quality for manufacturers. This mutually-beneficial collaboration can only exist if users can replace their firmware on their router with a customized version of OpenWrt. By preventing firmware replacement, these regulations will strangle this community in the US thereby increasing costs to hardware manufacturers which could be passed along to customers and employees.

Guest Wifi hotspots businesses

Additionally, many companies, such as ones involved in creating open wireless networks for retail locations would be hampered by these regulations. Currently, many of these companies install custom firmware on off-the-shelf hardware. Under these regulations, such companies would have to either create their own hardware, an expensive proposition for small software businesses, or receive authorization from a manufacturer under any arbitrary terms the manufacturer so chooses.

Commercial VPN services businesses

Many commercial VPN providers sell wireless routers as part of there product offerings. Denying companies and users the option to purchase more secure routers with support for VPN services will put a variety of users at risk.

Emergency Preparedness

Emergency preparedness would be hindered by restrictions on the modification of router hardware. Mesh networking is a key component of disaster response in our modern world. In disasters, amateur radio operators create mesh networks for disaster response. These operators use firmware like Broadband-Hamnet to create mesh networks on low-cost commodity routers operating at frequencies and power levels legally authorized for hams but not for other users. By modifying the device in such ways, wireless networks can be organized to cover much larger swaths of area to first-responders and emergency personnel. These restrictions would delay the exchange of emergency information and put lives at risk. The value of modified router hardware to assist in disaster response is recognized by emergency managers. In 2013, the International Association of Emergency Managers [6] designated Broadband-Hamnet as their US Technology and Innovation Award winner and Global Technology and Innovation Award winner.

Security

Restrictions on replacing router software will have a serious impact on security. Manufacturers are notoriously lax about providing timely security updates where such updates are provided at all. Security experts routinely recommend users replace manufacturer shipped router firmware with alternative community driven versions as a solution to this problem. In a recent security review of commercial routers, every one had critical security vulnerabilities. In most security instances replacing router firmware with third party peer reviewed firmware is the only option to solving this type of problem. While the security dangers for home users are serious, for large companies security dangers are critical. Without the ability to replace this software, large companies purchasing routers are entirely at the whim of the router maker. If this software is insecure, whether accidentally or intentionally, large American companies will be put at risk of industrial espionage.

Thanks,

Braxton.